<u>IN THE CLAIMS</u>

This listing of claims will replace all prior versions and listings of claims in the Application:

<u>LISTING OF CLAIMS:</u>

1. (Currently Amended) A dynamic file access control and management system configured to access one or more content sources, including a set of content, said system comprising:

     A.   a proxy system linked to said one or more content sources, said proxy system comprising an access control module configured to selectively obtain content comprising data blocks from said content sources on an individual block basis as a function of an authorization of a user requesting said content and a set of access policies comprising a set of predefined usage policies associated with said content for said user;

     B.   a rights management module configured to generate a set of usage rights associated with said content as a function of the set of predefined usage policies associated with said content for said user;

     C.   at least one client device having a client module configured to interface to a client operating system kernel, said client module configured to enforce the set of usage rights within the operating system kernel without application rewrites<u>, wherein enforcing the set of usage rights within the operating system kernel includes:</u>

          <u>intercepting a system call between an application and the client operating system;</u>

          <u>evaluating the system call based on the set of usage rights; and</u>

          <u>optionally blocking or modifying the system call based on said evaluation</u>; and

D.   one or more communication means, via which said content and said usage rights are provided to said client device.

2. (Previously Presented) The system according to claim 1, wherein said content and said usage rights are provided to said client device via different communication means.

3. (Previously Presented) The system according to claim 1, wherein said content includes static content.

4. (Previously Presented) The system according to claim 1, wherein said content includes dynamic content.

5. (Previously Presented) The system according to claim 1, wherein said communication means includes a secure transform configured to encrypt and encapsulate said content into a message as a function of a session ID and said client is configured to extract said content from said message.

6. (Previously Presented) The system according to claim 1, wherein said proxy system further includes a user interface, configured to facilitate creation and editing of said access policies and said usage policies and association of said access policies and said usage policies with said content.

7. (Previously Presented) The system as in claim 1, wherein said client device is a device from a group comprising:

1)   a personal computer;
2)   a workstation;
3)   a personal digital assistant;
4)   an e-mail device;
5)   a cellular telephone;

      6)   a Web enabled appliance; and

      7)   a server.

8. (Original) The system of claim 1, wherein said proxy system and at least one of said content sources are hosted on the same computing device.

9. (Currently Amended) A method of dynamic access control and management of content, the method comprising:

    A.   to content comprising data blocks accessible from a set of content sources on an individual block basis as a function of an authorization of a user requesting said content and a set of access policies comprising a set of predefined usage policies associated with said content for said user by a proxy system, correlating one or more user and/or client device identifications and defining the set of usage policies, wherein for the content said usage policies relate to selectively enabling or disabling operations associated with said content;

    B.   by said proxy system, generating a set of usage rights associated with the content as a function of the set of usage policies associated with said content and the one or more user and/or client device identification;

    C.   communicating said content and said usage rights to a client device associated with said one or more user and/or client device identification; and

    D.   using a client module at said client device and configured to interface to a client operating system kernel without application rewrites, enforcing the set of usage rights within the operating system kernel, wherein enforcing the set of usage rights within the operating system kernel includes:

          intercepting a system call between an application and the client operating system;

<u>evaluating the system call based on the set of usage rights; and</u>

<u>optionally blocking or modifying the system call based on said evaluation</u>.

10. (Previously Presented) The method of claim 9, wherein in step C, said communicating is accomplished by communicating said content and said usage rights to said client device via different communication means.

11. (Previously Presented) The method of claim 9, wherein said content includes static content.

12. (Previously Presented) The method of claim 9, wherein said content includes dynamic content.

13. (Previously Presented) The method of claim 9, wherein said communicating is accomplished using a communication means that includes a secure transform, including encrypting and encapsulating said content into a message as a function of a session ID and said client device is configured to extract said content from said message.

14. (Previously Presented) The method of claim 9, wherein said proxy system further includes a user interface and step A include creating and/or editing said access policies and said usage policies and associating said access policies and said usage policies with said content using said user interface.

15. (Previously Presented) The method of claim 9, wherein said client device is a device from a group comprising:

      1)   a personal computer;

      2)   a workstation;

    3)   a personal digital assistant;

    4)   an e-mail device;

    5)   a cellular telephone;

    6)   a Web enabled appliance; and

    7)   a server.

16. (Previously Presented) The method of claim 9, further comprising hosting said proxy system and at least one content source on the same computing device.